CLAIMS-

What is claimed is:

1. A method for safely executing downloaded code on a computer system comprising:

accessing an application process wherein said application process makes a system call to a library of said computer system for a resource, establishing a requesting thread;

sending a request message from said library to a local security filter;

validating said requesting thread at said local security filter and returning a digital signature that uniquely identifies said requesting thread to said application process; and

making a system call from said application process to a kernel of said computer system wherein said kernel uses said digital signature from said security filter to validate said requesting thread before allowing access to said resource.

2. The method as recited in Claim 1 further comprising

sharing a secret between said security filter and said kernel wherein said secret is used by said security filter to generate said digital signature and is used by said kernel to validate said digital signature.

3. The method as recited in Claim 1 wherein said library is a standard ntdll.dll library.

4. The method as recited in Claim 1 further comprising:

restricting said security filter to an address space that is not accessible by said application.

5. The method as recited in Claim 1 further comprising:

said kernel denying access to said resource if said digital signature can not be validated.

6. The method as recited in Claim 1 further comprising:

downloading executable code initiating said application process.

7. The method as recited in Claim 1 further comprising:

modifying said kernel such that only system calls that pass through said local library are allowed by said kernel.

8. The method as recited in Claim 1 further comprising:

restricting access of said application process to said resource for one command based on said digital signature.

9. The method as recited in Claim 8 further comprising:

restricting access of said application process to said resource for one time based on said digital signature.

10. A method for determining the source of a resource request comprising:

accessing a resource request associated with an application;

routing said resource request to a security filter, said security filter comprising a validation secret;

validating said resource request at said security filter and generating a first check value associated with said resource request using said validation secret;

routing said resource request to a system kernel wherein said system kernel comprises said validation secret;

generating a second check value associated with said resource request based on said validation secret at said system kernel; and

allowing access to said resource if said first check value and said second check value match.

11. The method as recited in Claim 10 further comprising:

denying access to said resource if said first check value and said second check value are different.

12. The method as recited in Claim 10 further comprising:

storing said first check value in a secure address space that is not accessible to said application.

13. The method as recited in Claim 12 further comprising:

said system kernel retrieving said first check value from said secure address space.

14. The method as recited in Claim 10 wherein said first check value is a digital signature.

15. The method as recited in Claim 10 further comprising:

restricting access of said application to said resource for a single resource request.

16. The method as recited in Claim 10 further comprising:

restricting access of said application to said resource for a single time.

17. The method as recited in Claim 10 further comprising:

allowing only resource requests that pass through said security filter to be processed by said system kernel.

18. The method as recited in Claim 10 further comprising:

downloading executable content using said application.

19. The method as recited in Claim 10 further comprising:

modifying said kernel such that only system calls that pass through said security filter are processed by said kernel.

20. A computer system for making it safe to execute downloaded code comprising:

a modified local library associated with an application, said local library coupled to a security filter wherein said security filter comprises a secret for generating a first digital signature associated with a resource request from said application; and

a system kernel for processing said resource request, said system kernel comprising said secret for generating a second digital signature associated with said resource request wherein said kernel denies said resource request if said first digital signature and said second digital signature are different.

21. The system as recited in Claim 20 wherein said application is a web browser.

22. The system as recited in Claim 20 wherein said local library is a ntdll.dll library.

23. The system as recited in Claim 20 wherein said security filter is located in an address space that is not accessible by said application.

24. The system as recited in Claim 20 wherein said digital signature verifies that said resource request originated from said local library.

25. The system as recited in Claim 24 wherein said system kernel distinguishes between resource requests that come from said local library and resource calls that come from outside said local library wherein only resource calls that come from said local library are processed.